



Mission Support Alliance

Statement of Work

Title: Cyber Security Analyst

Revision Number: 0

Date: November 7, 2016

1.0 INTRODUCTION / BACKGROUND

MSA operates a computer network on the Hanford Site called the Hanford Federal Cloud (HFC) for the United States Department of Energy (DOE). MSA Cyber Security manages the cyber security program for DOE and is the organization responsible for the protection of the network and the information it contains. In performing this essential role on the HFC, MSA Cyber Security carries out projects and activities involving intrusion detection, incident response, penetration testing, application security, network segmentation, vulnerability remediation, risk mitigation, personally identifiable information, and industrial control system security.

The Subcontractor is required to provide staff augmentation support as set forth herein:

2.0 OBJECTIVE

MSA Cyber Security is responsible for managing the cyber security program at Hanford in accordance with the Federal Information Security Management Act (FISMA) and National Institute of Standards and Technology (NIST) requirements for operation of federal information systems. For a program of this size and complexity, the organization must augment its staff with an engineer/analyst to assist in supporting the program and associated projects to ensure continued compliance with cyber security requirements.

3.0 DESCRIPTION OF WORK – SPECIFIC

Perform engineering and analysis activities in cyber security, supporting oversight of information technology throughout the enterprise. Provide technical support to assess software applications for the protection of personally identifiable information (PII). Conduct privacy needs assessments and privacy impact assessments on unclassified information systems, including determining PII applicability and evaluating system protections in place for handling PII to mitigate privacy risks. Support system owners in completing information system assessments. Coordinate with information technology staff members to analyze database content and organization. Identify and implement cyber security controls to restrict access to PII in applications. Participate in disaster recovery exercises and events. Assess and mitigate security threats and risks to computer



Mission Support Alliance

systems. Participate in development of the System Security Plan (SSP) for the Hanford Federal Cloud (HFC) under National Institute of Standards and Technology (NIST) requirements. Support secure operation and maintenance of systems within accreditation boundary. Participate in change management process for information systems. Support cyber security audits, assessments, data calls, and investigations.

4.0 QUALIFICATIONS

Subcontractor shall ensure that its personnel meet and maintain the appropriate training, qualifications, and certification requirements as applicable.

Basic Qualifications

- BA/BS degree in Computer Science or a related field plus 10 years of experience working in information technology, or BA/BS degree in another field plus 12 years of experience working in information technology.
- In addition, 2 years of recent experience working in cyber security.
- Proven experience in analyzing complex software applications, database schemas, and information flows.
- Demonstrated systems analysis capability to apply the requirements of DOE O 206.1, Department of Energy Privacy Program, to information systems.
- Knowledge of National Institute of Standards and Technology (NIST) requirements for operation of federal information systems.
- Demonstrated ability to develop and apply cyber security policies and procedures.
- Experience in assessing and managing risk from a cyber-security perspective, especially related to personally identifiable information (PII).
- Ability to set and manage priorities judiciously.
- Excellent written and oral communication skills, interpersonal skills, and strong negotiating skills.
- Ability to present cyber security and PII concepts and ideas at an appropriate level to system owners, users, and executives responsible for business decisions.
- Exceptionally self-motivated and directed.
- Keen attention to detail.
- Superior analytical and problem solving abilities.
- Exceptional service orientation.
- Ability to motivate personnel in a team oriented, collaborative environment.

Desired Qualifications

- Advanced degree in Computer Science or a related field.
- Experience with information technology on the Hanford Site.
- Certification as a Certified Information Systems Security Professional (CISSP).



Mission Support Alliance

5.0 REQUIREMENTS

General

Subcontractor shall operate in accordance with MSA policies, procedures, and processes. MSA will supervise and direct the day to day work activities of the Subcontractor's personnel.

For any work performed on the Hanford Site or in any MSA controlled facility, the provisions of the On-Site Services Special Provisions will apply to Subcontractor personnel.

5.1 Engineering Requirements

APPLICABLE ENGINEERING CODES AND STANDARDS

Number	Title
DOE O 206.1	Department of Energy Privacy Program http://www.directives.doe.gov/directives-documents/200-series/0206.1-BOrder
NIST SP 800-53 Revision 4	Security and Privacy Controls for Federal Information Systems and Organizations http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

5.2 Environmental, Safety, & Health Requirements

The Subcontractor shall perform work safely, in a manner that ensures adequate protection for employees, the public, and the environment, and shall be accountable for the safe performance of work. The Subcontractor shall comply with, and assist the Buyer in complying with environmental and safety requirements of all applicable laws, regulations and directives.

The Subcontractor shall exercise a degree of care commensurate with the work and the associated hazards. The Subcontractor shall ensure that management of environmental and safety functions and activities is an integral and visible part of the Subcontractor's work planning and execution processes. As a minimum, the Subcontractor shall:

- Thoroughly review the defined scope of work;
- Identify hazards and environmental and safety requirements;



Mission Support Alliance

- Analyze hazards and implement controls;
- Perform work within controls; and
- Provide feedback on adequacy of controls and continue to improve safety management.

The Subcontractor shall flow down all environmental and safety requirements to the lowest tier Subcontractor performing work on the Hanford Site commensurate with the risk and complexity of the work.

5.3 Quality Assurance Requirements

None.

5.4 Government Property

None.

6.0 PERSONNEL REQUIREMENTS

6.1 Training

- A. Hanford site-specific general training requirements to safely perform this work will be designated by the Buyer's Technical Representative (BTR).
- B. The following types of training qualifications are required:
 - Hanford General Education Training (HGET)/MSA General Education Training (MGET) is required.
 - Other site specific training may be required as determined during performance of this scope of work.

6.2 Security and Badging Requirements

- A. For any on site work, see Special Provisions – On-Site Services for details.
- B. The Subcontractor shall wear a Buyer-issued security badge identifying themselves. A minimum of two working days advance notice is needed for site badging.
- C. Subcontractor employees will be required to submit to vehicle searches and not personally carry or transport certain prohibited articles.
- D. The Subcontractor will not require a security clearance.



Mission Support Alliance

- A security clearance is required for all Subcontractors who will have: (1) access to classified matter, (2) access Special Nuclear Material (SNM), and/or (3) require frequent, unescorted access to secured areas.
- A facility clearance must be in place at Hanford for the individuals employer (facility), before a security clearance may be granted Facility Clearance (FCL) approval will be required for a facility to be eligible to (1) access, handle or possess classified information, (2) SNM, or other hazardous material presenting a potential sabotage threat, or (3) responsibilities for safeguarding \$5M+ of government property. If any of these criteria apply to the SOW, the Contract Specialist needs to be notified immediately, in order to process clearance paperwork. The work cannot begin until an FCL is in place. A new FCL is required for each subcontract meeting the criteria.
- A subcontractor that will not possess classified information or matter, or SNM at the subcontractor's place of business and will only access such security activities at other cleared facilities must be cleared as a "non-possessing facility."

6.3 Work Location/Potential Access Requirements:

2261 Stevens, 1981 Snyder, 1979 Snyder, 2355 Stevens, MO404.

6.4 Site Access and Work Hours

Hanford personnel at the Hanford Site work a standard 4/10 schedule. The standard work week consist of ten (10) hours of work between 6:00 am and 4:30 pm, with one-half hour designated as an unpaid period for lunch, Monday through Thursday.

Work performed outside normal operating hours shall be coordinated and/or approved through the BTR and/or the Contract Specialist prior to performing the work.

7.0 MEETINGS, SUBMITTALS

Subcontractor shall participate in all meetings as required by the Buyer's Technical Representative (BTR).

8.0 SCHEDULE REQUIREMENTS

8.1 Schedule

Start date: **November 28, 2016** Completion date: **September 30, 2017 ***



Mission Support Alliance

(Buyer may exercise one or more options by providing written notice to the Subcontractor prior to the most current Subcontract end date. Lacking written notice by the Buyer, the option(s) will expire with the Subcontract).

* With two option periods to extend on an annual basis through September 30, 2019

Option Period 1: 10/1/2017-09/30/2018

Option Period 2: 10/1/2018-09/30/2019